Amendments to the Claims:

The following listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Canceled)

2. (Previously Presented) The information processing device of claim 19 wherein an expiration date is not set for the second encryption key.

3. (Previously Presented) The information processing device of claim 19 wherein the data input interface also inputs unencrypted data, and the encryption module also encrypts unencrypted data input by the data input interface.

4. (Previously Presented) The information processing device of claim 19 further comprising:

a key generator for generating the second encryption key.

5. (Previously Presented) The information processing device of claim 4, further comprising:

volatile memory; and

a memory controller for storing the second encryption key in the volatile memory.

6. (Previously Presented) The information processing device of claim 4, wherein the key generator generates the second encryption key using information characteristic to the device itself.

7. (Previously Presented) The information processing device of claim 4, wherein the key generator generates the second encryption key when power to the device is turned on.

8. (Previously Presented) The information processing device of claim 4, further comprising:

a media reader capable of being installed with a removable portable storage media storing key generation parameters for reading a key generation parameter stored on the installed portable storage media, wherein the key generator generates the second encryption key using the key generation parameter.

9. (Previously Presented) The information processing device of claim 4, further comprising:

a device for setting a security level for the information processing device; and

a device for storing the security level of the information processing device, wherein the key generator generates the second encryption key of a key length corresponding to the security level.

10. (Previously Presented) The information processing device of claim 4, further comprising:

a device for receiving settings for a region where the device is to be used; and

a device for storing the settings for the region of the information processing device, wherein the key generator generates the second encryption key of a key length corresponding to the region.

11. (Previously Presented) The information processing device of claim 19 further comprising:

a media reader capable of being installed with a removable portable storage media storing the encryption key, wherein the encryption module reads the second encryption key from the portable storage media installed in the media reader and performs encryption.

12. (Previously Presented) The information processing device of claim 19 equipped with a plurality of the storage devices, and having second encryption keys corresponding to each storage device, wherein the encryption module performs encryption

using the second encryption key corresponding to storage device decided by a data storage destination.

13. (Previously Presented) The information processing device of claim 19 having encryption keys corresponding to each user using the device, wherein the encryption module performs encryption using an encryption key for the user corresponding to the data.

14. (Canceled)

15. (Previously Presented) The information processing device of claim 19 wherein the deciding device decides to encrypt encrypted data inputted by the data input interface and decrypted by the decryption module.

16. (Previously Presented) The information processing device of claim 19 further comprising:

a printer for decrypting and printing data stored in the storage device.

17. (Canceled)

18. (Previously Presented) The information processing device of claim 20 further comprising a step of:

storing the second encryption key in the volatile memory.

19. (Currently Amended) An information processing device, comprising:

a data input interface for inputting an input data that is one of an encrypted data and a non-encrypted data;

a decryption module for decrypting the encrypted data;

an encryption module for encrypting data that has been decrypted by the decryption module or the non-encrypted data;

a storage device for storing data; and

a deciding device for deciding whether the input data is ~~encrypted,~~encrypted data, whether to store the input data and whether to encrypt data decrypted by the decryption module,

wherein the decryption module decrypts the encrypted data ~~input by the data input interface~~ using a decryption key forming a pair with a first encryption key used to encrypt the encrypted data input by the data input interface,

the encryption module encrypts the decrypted data, which ~~is~~ has been decrypted by the decryption module, decided upon for encryption by the deciding device using a second encryption key different from the first encryption key,

the storage device stores the encrypted data encrypted by the encryption module and the non-encrypted data decided upon for storing by the deciding device,

the deciding device decides that the decrypted data decrypted by the decryption module and the non-encrypted data is either to be printed without the encryption module encrypting the decrypted ~~data,~~data or the non-encrypted data, or to be stored in the storage device, based on a job classification information of the decrypted ~~data,~~data and the non-encrypted data, respectively, and

the deciding device decides that:~~that~~

the decrypted data decrypted by the decryption module is to be at least one of: (i) stored in the storage device ~~either~~ with ~~or without~~ the encryption module encrypting the decrypted data and (ii) stored in the storage device without the encryption module encrypting the decrypted data when the deciding device decides that the decrypted data is to be stored in the storage device, based on a storage time and a confidentiality of the decrypted data, and~~data.~~

the non-encrypted data is to be at least one of: (i) stored in the storage device with the encryption module encrypting the non-encrypted data and (ii) stored in the

storage device without the encryption module encrypting the decrypted data when the deciding device decides that the non-encrypted data is to be stored in the storage device, based on a storage time and a confidentiality of the non-encrypted data.

20. (Currently Amended) A method for storing data inputted to an information processing device, comprising:

inputting an input data that is at least one of encrypted data and non-encrypted data;

decrypting the input data if the input data is encrypted data;

~~encrypting data;~~

~~storing data; and~~

deciding whether the input data is ~~encrypted,~~ encrypted data, whether to store the input data and whether to encrypt data that has been decrypted;

deciding based on a job classification information of the decrypted data and the non-encrypted data that the data that has been decrypted and the non-encrypted data is to either be printed without encrypting the decrypted ~~data;~~data or the non-encrypted data or the data that has been decrypted or the non-encrypted data is to be stored;

deciding based on a storage time and a confidentiality of the decrypted data and non-encrypted data ~~that~~ that:

the data that has been decrypted is to be at least one of: (i) stored ~~either~~ with ~~or without~~ encrypting the decrypted data and (ii) stored without encrypting the decrypted data when it is decided that the decrypted data is to be ~~stored;~~stored, and

the non-encrypted data is to be at least one of: (i) stored with encrypting the non-encrypted data and (ii) stored without encrypting the non-encrypted data when it is decided that the non-encrypted data is to be stored; and

instructing to execute a print process associated with the inputted data after deciding that at least one of: (i) the data that has been decrypted is to be printed without encrypting the data, and (ii) the non-encrypted data is to be printed without encrypting the data, wherein:

~~wherein~~ a decryption module decrypts encrypted data input by a data input interface using a decryption key forming a pair with a first encryption key used to encrypt the data,

an encryption module encrypts data decided upon for encryption by a deciding device using a second encryption key different from the first encryption key,

a storage device stores data decided upon for storing by the deciding device, and

the decryption module decrypts encrypted data encrypted by the encryption module and stored in the storage device using the second encryption key.

21. (Previously Presented) The information processing device according to claim 19, wherein deciding whether to store the input data is based on a job classification information of the input data.

22. (Previously Presented) The information processing device according to claim 19, wherein deciding whether to store the input data is based on a time of job processing information of the input data.

23. (Previously Presented) The information processing device according to claim 19, wherein deciding whether to encrypt data decrypted by the decryption module is based on attribute information of the input data.

24. (Previously Presented) The information processing device according to claim 19, wherein deciding whether to encrypt data decrypted by the decryption module is based on a confidentiality information of the input data.

25. (Previously Presented) The information processing device according to claim 19, wherein deciding whether to encrypt data decrypted by the decryption module is based on a storage time of the input data.

26. (Previously Presented) The information processing device according to claim 19, wherein deciding whether to encrypt data decrypted by the decryption module is based on a comparison of at least one of a confidentiality information of the input data or a storage time of the input data to a predetermined threshold value.

27. (Previously Presented) The information processing device according to claim 19, wherein deciding whether to encrypt data decrypted by the decryption module is based on instruction data provided with the input data.

28. (Previously Presented) The information processing device according to claim 19, wherein deciding whether to encrypt data decrypted by the decryption module is based on security data that represents a level of security of the storage device.

29-30. (Canceled)